International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: https://www.tandfonline.com/loi/ujic20

Iranian Counterintelligence

Carl Anthony Wege

To cite this article: Carl Anthony Wege (2019) Iranian Counterintelligence, International Journal of Intelligence and CounterIntelligence, 32:2, 272-294, DOI: 10.1080/08850607.2019.1565274

To link to this article: https://doi.org/10.1080/08850607.2019.1565274

Published online: 09 May 2019.

International Journal of Intelligence and CounterIntelligence, 32: 272–294, 2019

ISSN: 1521-0561 print/0885-0607 online
DOI: 10.1080/08850607.2019.1565274

CARL ANTHONY WEGE

Iranian Counterintelligence

Counterintelligence disciplines are, by their nature, more obscure than the larger community of analytic disciplines. Only a very few professionals, such as Michelle Van Cleave, John Ehrman, and Cynthia Grabo, have produced open literature materials with a primary focus on counterintelligence.[1] Iranian counterintelligence (CI) activity remains almost unaddressed, leaving a significant gap in the open literature.

In contrast to democratic countries, where intelligence services are configured to inform the decisionmaking process of political leaders, Near Eastern intelligence organizations often pursue different purposes. In many Arab countries multiple *Mukhābarāts* are structured for the dual purpose of repressing popular dissent and preventing any *coup d'état*. Consequently, the foundation of many such Mukhābarāts is regime preservation rather than educating political decisionmakers. Iranian intelligence and counterintelligence organs share similarities of purpose with the Arab Mukhābarāts while having distinctive permutations drawn from Persian sociology and the history of Iran.

IRAN'S INTELLIGENCE ARCHITECTURE

Iran's modern intelligence architecture begins with Shah Mohammad Reza Pahlavi's creation of *SAVAK* (Sazemn-I Eitela'at a Amniyat-I Kishavr) in 1957. In the immediate aftermath of Iran's 1979 Revolution, the Palestine

Carl Anthony Wege in early 2017 became Emeritus Professor of Political Science at the College of Coastal Georgia, Brunswick, where he had taught since 1989. A graduate of Portland (Oregon) State University, with an M.S. from the University of Wyoming, Professor Wege has written extensively on Middle East issues in a wide range of academic and professional journals.

Liberation Organization's (Fatah) intelligence entity *Jihaz al-Razd* provided some intelligence support for Ayatollah Ruhollah Khomeini's regime,[2] followed by the creation of *SAVAMA* (Sazman-e Ettelaat Va Amniat Meli) under the auspices of General Hussein Fardust as the first iteration of a post-Revolutionary Iranian intelligence enterprise. SAVAMA itself quickly transitioned into a Ministry of Intelligence and Security (MOIS, Vezarat-e Ettela'at va Amniat-e Keshvar or VEVAK) in 1984.[3] Ayatollah Khomeini's vision of the *Vilayat-e Faqih*[4] animating the Revolution created new standards wherein every Minister of Intelligence, beginning with Mohammed Rayshahri, was a religious authority rather than an intelligence professional.[5] Concurrently some of the educational institutions congruent with this vision, such as the Madrase-ye Haqqani theological school in Qom[6] and Imam Mohammed Bagher University in Tehran,[7] became associated with MOIS.

Ali Fallahian's appointment as Iran's Intelligence Minister in 1989 breathed life into a substantive Iranian intelligence organization that was setting up training agreements with Bonn, Moscow, and North Korea and installing then-modern Japanese communications equipment for use by the Intelligence Ministry.[8] MOIS, maturing in the 1990s, established a liaison relationship with the Russian Foreign Intelligence Service (Sluzhba Vneshnei Razvedki or SVR) which replaced the U.S. Central Intelligence Agency (CIA) and Israeli MOSSAD personnel who had educated the SAVAK in the 1960s and 1970s.[9] Russian tradecraft (including counterintelligence) manifested in a Persian cultural milieu came to define the foundations of Iranian intelligence. In the mid-1990s MOIS adopted a model pioneered by Russia's Yevgeni Primakov in revamping the SVR that was intended, in part, to restructure the Iranian service to better focus on counterespionage.[10] MOIS personnel were trained in traditional Soviet KGB tradecraft and the old KGB methods of disinformation which the MOIS called *Nefaq* (an Arabic, not Farsi, word for "discord" or "hypocrisy"). That "hypocrisy" was made congruent with the concept of *Taqiyya* or *Kitmān* in Tehran's information operations promoting the *Vilayet* across the region.[11] The French Centre for Research on Intelligence estimated that the MOIS was employing roughly 15,000 persons a decade ago, with a significant percentage deployed overseas under both official and non-official cover.[12] The maturing MOIS administrative structure was, by the 1990s, conforming to that found in many other intelligence agencies, with multiple directorates exercising traditional functions.[13] More recent iterations of the MOIS under Mahmoud Alavi have evolved less as a traditional Ministry but rather more akin to an executive body by-passing the President and reporting directly to the Supreme Leader of the Islamic Republic, Ali Hosseini Khamenei.[14]

Throughout the bitter combat of the 1980s Iran–Iraq War Ayatollah Khomeini kept alert to the counter-revolutionary potential he saw in the

armed forces. Concurrent with the growth of MOIS and distrustful of the imperial foundations of the military Artesh, the House of the Leader (Beyt-e Rahbari) continually enhanced the authority of the Iranian Revolutionary Guard Corps (Sepāh-e Pāsdārān-e Enqelāb-e Eslāmi, Sepah, Pasdaran, or IRGC) as a counterweight to the Artesh. To suppress counter-revolutionaries, the representative of the Supreme Leader in the Armed Forces instituted what amounted to a "commissar system" of clerics at every level of the armed forces, the IRGC, Basiji, and the Defense Ministry with the task of identifying personnel whose propensities might tarnish what supporters of Iran's Revolution would consider as the quintessential pearl of the *Vilayat-e Faqih*.

Any Weberian understanding of Iran's formal organizational structures is only partially descriptive and of limited utility when describing its larger intelligence apparatus.[15] Lines of authority do not necessarily always run vertically though organizations but can extend laterally between them.[16] Likewise, while Iranians are reasonably good at collecting intelligence they are lacking in analyzing that which was gathered at the national level. The products of intelligence analysis are relayed to political leaders through a Shi'a Islamist veneer designed to placate the scholar–jurists by giving undo weight to convoluted conspiracies often involving Jews and the Baha'i rather than in realistic assessments and key judgments that might doom an objective analyst to the potential charge of "Occidentosis" (*Gharbzadegi* or Western intoxication).[17]

THE TOP OF THE STRUCTURE

The apex of Iran's official national security establishment, the Supreme National Security Council (SNSC), is intended to aggregate policymakers and the heads of the security apparatus and the armed forces into a coherent governing body. Yet, the SNSC's organization serves less as a rational structure reflecting formal administration in a Weberian sense, able to be informed by and act on actionable intelligence, but rather as an arena for political contests and negotiations. It is a constellation of factions and crisscrossing reporting lines with authority anchored in patron–client relationships and *Dowreh*[18] groups spanning multiple Shi'a power centers, Bonyads, and financially self-sufficient religious organizations. The SNSC at this juncture does not appear to have any secondary bodies equivalent to the U.S. National Counterintelligence Executive,[19] and the concept of Strategic Counterintelligence such as advocated for the United States by Michelle Van Cleave seems less developed within Iran's counterintelligence system. Iranian counterintelligence appears fractured across multiple organizations and uncoordinated at a national level, and defined by an ad hoc and case-driven approach.[20] Having a Van Cleave–like 'strategic counterintelligence' vision

might suggest to Tehran the impact of corruption across Iran's CI ecosystem, which would result in a more strategically coherent approach, but Iran still apes the traditional *ad hoc* case system which is to Tehran's disadvantage.

But, operationally, the case-driven Iranian approach to counterintelligence can remain functional. For example, several years ago, a CIA operation that was apparently making a shotgun effort to recruit a wide variety of Iranian nationals, who might someday have access to information targeted for intelligence collection and who had left the country for business in Malaysia, was compromised using such a case-driven approach. One of the students pitched by the CIA apparently reported the recruitment attempt to Iranian authorities in Iran. Thereafter, MOIS was able to identify both some two dozen students and other nationals who failed to report the Agency's recruitment efforts and a significant number of CIA operations officers.[21] If, in fact, MOIS rolled up this nascent network as publicly described, its case-driven approach to counterintelligence seems able to identify and respond to foreign recruitment efforts, and capable of separating indicators of a genuine recruitment attempt from false recruiting reports based on corrupt reporting, misunderstanding, or personal delusions.

THE PASDARAN

In the last couple of decades, the Pasdaran has emerged as a Praetorian Guard and now constitutes the political and security backbone of the Islamic Republic. As the Guard continued to consolidate power it was given responsibility for Iran's nuclear programs,[22] and as Iran approached the status of a nuclear threshold state its programs were targeted for extensive covert operations by adversary services.[23] In 2005, the *Oghab 2* (Eagle 2) organization, initially headed by Ahmad Wahidi,[24] was announced under IRGC auspices as a distinct body tasked with the protection of Iran's nuclear assets, including the guarding of senior scientists and engineers, industrial equipment across the nuclear program, and the information infrastructure supporting it.[25] The Oghab 2 employee component apparently doubled during 2008 following a number of successful assassinations that disrupted Tehran's nuclear program along with major sabotage incidents at Khavarshahar and Kavir Lut.[26] In 2009 President Mahmoud Ahmadinejad tasked General Abdulreza Chahili with yet again restructuring and reorganizing Oghab-2, a task which General Chahili turned over to a former member of Iran's Supreme National Security Council, General Ali Hosain Tach.[27] The organization now includes a discrete psychological warfare and disinformation department to obscure elements of the nuclear program. Formally under the Guard, with several thousand employees, it apparently reports laterally to the MOIS Counterintelligence Directorate.[28]

Following the near domestic uprising over Iran's fraudulent elections in 2009 the Khamenei government reorganized many security agencies, including several associated with the IRGC. Khamenei decreed creation of a new entity, called the Intelligence Organization of the Islamic Revolutionary Guard Corps (Sazeman-e Hefazat va Ettelaat or SHE) which reorganized the existing cadre of officers and managers in order to populate the new organization. The IRGC Intelligence Organization, headquartered at Qasr-e Firouzeh in Kamali near Tehran, is now headed by Hojatoleslam Hossein Taeb, with Gholamhossein Ramazani serving as his counterintelligence chief.[29] Taeb's IRGC Intelligence Organization also commands the Internal Security Directorate at MOIS and the security apparatus of the Basiji. Taeb's role again illustrates a matrix of reporting lines crossing agency jurisdictions thereby obscuring the functional relationships between Iranian intelligence bodies.

Both the MOIS and the IRGC operate a network of prison and detention facilities, or portions thereof, both formal and informal, serving their own intelligence and counterintelligence interests and missions. For example, in the well-known Evin Prison near Tehran the IRGC controls Ward 2A and Section 325[30] along with the Tawhid Detention Center. Evin's Ward 209 serves as the main MOIS detention center, where persons are held while initial investigations of intelligence relevance are completed.[31] Prison 59 (Eshratabad), also in Tehran, is specifically used by the IRGC Intelligence Organization. Additionally, semi-secret prisons run by Artesh Intelligence are Detention Center 36 (Jamshidyyih and Hishmatiyyih), and the Ministry of Defense Intelligence Protection Organization maintains its own prison, called Jay.[32] These are separate from the traditional prisons operated by the Judiciary, such as Tehran's Kahrizak Detention Center, which was also used for political prisoners and ultimately was ordered closed. Iran's State Prisons Organization, now headed by Asgar Jahangir, a former Chief of the Judiciary's Counterintelligence Organization,[33] has no legal jurisdiction over the MOIS and IRGC-controlled elements of the detention system.

The Iranian government was described here earlier as a constellation of factions, competing power centers, patron–client relationships, and multiple Dowreh groups. This also describes the functioning of the formal organizational structures of the MOIS and IRGC which precipitates conflicts difficult to regularize through formal organizational channels. The House of the Leader, a significant traditional center of power in Iran, acts as an administrative office answering directly to the Supreme Leader (Rahbar). Ayatollah Khamenei has expanded this body and tried to utilize it to institutionalize conflict management between the MOIS and IRGC through an administrative device called Department 101, which acts as a special intelligence entity under Asghar Mir Hejazi. He also commands a special unit

of the Revolutionary Guard, the Sepah-e Vali Anr, which protects the Supreme Leader, arbitrates conflict, clarifies responsibilities, and coordinates some intelligence activities between MOIS and the IRGC.[34]

IRANIAN COUNTERINTELLIGENCE

Counterintelligence nomenclature, whether applied in an Iranian context or elsewhere, is somewhat malleable, and the semantics of its usage change in time and across cultures. Terms and phrases like defensive and offensive counterintelligence, strategic counterintelligence, and distinctions between security and counterintelligence, can be soft distinctions. Best practice would acknowledge that intelligence and counterintelligence disciplines have definitive nomenclatures, but that semantic squabbles are cross-culturally problematic anyway so they should not dissuade a conceptual discussion of Iranian CI.[35] A basic theoretical definition of counterintelligence suggests that "Counterintelligence refers to information gathered, and activities conducted to protect against espionage (and) other intelligence activities. …"[36] Counterintelligence can be viewed as an analytic discipline (it is also considered an operational discipline and reasonable people can here agree to disagree) that has as its foundational objective the countering of the activities of foreign intelligence services. That objective can be achieved through various methods including deception, penetration of hostile services, ferreting out threats within one's own services, and looking for broader efforts to subvert civil society.[37] Organizationally, CI can be a component of the positive overall collection effort. It can also be segmented into a stand-alone organization, or blended into the larger intelligence architecture using both approaches. In general, the open literature on counterintelligence nomenclature often conflates relevant terms thereby creating unintended obfuscation. This can be a function of viewpoint, as a single event that might be considered positive human intelligence collection may also be considered an offensive counterintelligence operation from a different perspective.

Like all governments, Iran has its unique ways of incorporating the counterintelligence function into the screening of candidates for its security services. In Khamenei's government counterintelligence vetting begins as soon as candidates are recruited into the Iranian services. Selecting applicants for the Ministry of Intelligence and Security, the Revolutionary Guard, and the Basiji requires counterintelligence approaches specifically related to the structural and functional differences among the organizations. The most robust selection process, from a counterintelligence standpoint, is that of the MOIS. It begins with the recruitment of individuals having specific subject majors, with testing in Hamedan in western Iran, followed by nine- to twenty-four-month investigations, then by further specialized intelligence training at Tehran's Imam Bagher University, and an initial assignment to

relevant provincial intelligence offices.[38] By contrast, admission to the Revolutionary Guard is as simple as the enlistment option to fulfill one's military service obligations. That said, advancement in Guard ranks engages a more and more stringent counterintelligence examination of the religious and political views of candidates and their family members.[39] Entrance requirements for the Basiji are the least stringent, with entry into Basiji Student Organizations requiring little more than a photo ID, although constant monitoring by the Basiji at least creates an observable timeline for counterintelligence investigators from that point forward.

Iran's human and cultural terrain necessarily impacts its approach to this counterintelligence enterprise. Paraphrasing a literary idiom from Iran's ancient Master Narrative illustrates the cultural norms of this terrain: "In Iran there are counterintelligence organs; on the other hand there are no counterintelligence organs." The idiom is used in a narrative sense to convey the Persian cultural idea that there is really nothing other than Allah. Used here, it emphasizes the Iranian view that counterintelligence, like all things, must ultimately be in the hands of Allah. Structurally, Iranian CI is not limited to discrete organizations that can be administratively described in a Weberian sense, but is rather a mixture of stand-alone organizations and counterintelligence functions diffused across Iran's security matrix. That security matrix is wide and deep, but it is also amorphous, with varying densities in distinct organizations.

MILITARY COUNTERINTELLIGENCE

The military intelligence organ charged with Army counterintelligence, the Intelligence Protection Organization of the Islamic Republic of Iran (SAHEFAJA), utilizes an independent chain of command to report to the Supreme Leader. While the Commander-in-Chief's General Office of Counterintelligence (Daftar-e Omoumi-ye Hefazat va Ettelaat-e Farmandehi-e Kol-e Qova) formally sits at the apex of a CI system that includes the Ministry of Defense Counterintelligence Organization, the IRGC Counterintelligence Organization under Brigadier General Mohammed Kazemi[40] and the Law Enforcement Forces Counterintelligence Organization[41] are in many ways more significant to Iran's internal security.[42]

Tehran's CI system is operationally broad, and attempting to assess the external dimensions of offensive Iranian counterintelligence operations would be an attempt to describe too much with too little. A more productive purpose then is a description of internal security CI within the Islamic Republic itself. Like that of most aspirational powers, Iran's counterintelligence architecture has successfully contained and eliminated multiple threats to the regime. But whether Iran's successes were the result of Iranian prescience, sloppy tradecraft on the part of Tehran's adversaries,

luck, or some combination thereof probably does not much matter. A congruence between the public domain narrative that explains successful Iranian counterintelligence measures and an objective assessment of the basis for such success is problematic because the "chain of acquisition" in gathering information to judge those events is not directly observable. Since the public domain explanation is at least plausible, and perhaps in a few instances accurate, it may help illuminate the edges of Iranian counterintelligence accomplishments and how they materialized.

DEFECTORS AND COUNTERINTELLIGENCE

Defectors, and the art of understanding defectors in an Iranian context or any other, represent a special kind of counterintelligence challenge. While managing defectors is always problematic, the gathering of human intelligence (HUMINT) in denied areas is a complex endeavor and defectors offer the potential of real collection shortcuts.[43] The assessment of defectors, however, requires both unique and discrete counterintelligence analysis, and is still practiced as both art and science. Defectors in place (sometimes called agents in place) are of greater value to an adversary service, while an immediate defection and exfiltration is of lesser value as the information package the defector can betray to adversary services is thereby limited to past intentions, knowledge, operations, and practices.[44]

Typical of a "Second World" power under intense pressure from "First World" adversaries, Iran has suffered some painful defections, among them that of VEVAK co-founder Abu al-Kassam Misbahi who defected to the German BND (Bundesnachrichtendienst) in 1996. Likewise, the defection of former Deputy Defense Minister and Pasdaran Chief Ali Reza Ashgari, with his intimate knowledge of the foundation of Hezbollah, was disastrous. Ashgari had apparently served as an agent in place since 2003,[45] and his exfiltration from Istanbul, Turkey, in 2007 indicates careful planning and therefore implies adequate planning time. High level defections like this are effectively unthinkable in mature First World nations like Britain, Japan, and the United States, but they can happen in Second and Third World countries, and the possibility of such high-level defections must therefore be considered part of the CI ecosystem in countries like Iran.

Tehran has been reasonably effective in precluding the defection of diplomatic personnel in its foreign service, in part due to a potential for reprisal against family members remaining in Iran. In addition to such standard police state methods as informant networks, the newer social media surveillance methods look for evidence of disloyalty within the diplomatic corps. For example, the Pasdaran, after the 2015 nuclear agreement with the United States that remains controversial among Iranian hardliners, organized multiple "spear phishing" attacks against Iranian diplomats to both monitor

them and compromise their foreign service peer networks to the Guard.[46] From the time the Khomeini government consolidated power almost two generations ago, until the period following the fraudulent 2009 elections, Iran has experienced the defection of only some twenty diplomats to various countries.[47] But preventing defection is only part of the counterintelligence challenge. Iran's ability to protect its diplomatic and other codes against penetration by First World adversary services is fundamentally limited by Iran's status as a second level economic and technological power.[48] It simply does not have sufficient capacity to deploy the technological and human capital required to protect its communications systems across the board from its major international adversaries.[49] That said, Iran is able to protect some communications, thereby allowing many of its high priority foreign diplomatic operations some possibility of security.

Concurrently, Iran has also demonstrated the skills necessary to successfully target international organizations to further its political purposes. In its counterintelligence ecosystem, non-Iranian Shi'a designated by Iran's service can be targeted, using such Iran-based non-governmental organizations engaged in public diplomacy as lAbl-ul-Bayt World Assembly, for counterintelligence operations. *Abl-ul-Bayt,* which refers to the Household of the Prophet, was established as an organization headquartered in Tehran in 1990 as a global influence network promoting outreach to non-Iranian Shi'a and those who might be sympathizers to the Iranian Revolution. Its most recent conference in Tehran in 2015 drew roughly 1800 non-Iranian Shi'a from 130 countries.[50] The MOIS had not only the challenge of monitoring possible foreign intelligence officers and adversary service penetration operations among the attendees[51] but the opportunity for cultivating attendees for ongoing intelligence-related development.

Despite Tehran's wish that Iran be a denied area for adversary intelligence services, Iranian nationals, Iranian expatriates, and foreigners transverse the country's frontiers with some regularity. Its eighty-seven official border points complicate Iran's counterintelligence problems.[52] After the official points of entry the task of observing the intelligence affiliations of overt foreign entities that operate lawfully in Iran, ranging from foreign corporations to embassies, presents a strong challenge to Tehran's multiple security organizations. All-source analysis on those foreign entities and their acknowledged personnel, and incorporating their social media presence, creates a profile allowing for Iran to identify anomalies that may have intelligence relevance. That said, Iran like any power must prioritize its counterintelligence targets in a way congruent with both its resources and political objectives. Counterintelligence methods once used at Tehran's Imam Khomeini International Airport demonstrate the impact of limited resources. That airport's security system, in addition to traditional human spotters,[53]

utilized watch lists generated by both the IRGC and MOIS. When listed Iranian nationals and foreigners entered the country their movements and contacts could be mapped, and they could be arrested prior to departure, depending on the intent of the Iranian security organs.[54] Complicating that counterintelligence task is the reality that MOIS or the IRGC must be aware that individuals are of intelligence interest before their names can show up on an intelligence watch list. Iran's frontiers are volatile, and although invasion is difficult the counterintelligence environment becomes challenging, from the mountains populated by resisting and restless ethnic groups to the vast Dasht-e Lut deserts extending into Baluchistan,[55] making its porous borders inviting targets for foreign special operations. Given the impracticality of trying to seal the border from operations professionals the government's focus is on securing the population. Consequently, the focus of counterintelligence efforts is the population of the Mashhad region in the northeast[56] and the major population belt which runs from Tehran in the foothills of the El Burz range down toward the Zargos range and from there in the direction of the Strait of Hormuz.

Domestically, MOIS is the dominant security service, with specific responsibility to monitor Iran's ethnic minorities on the periphery of the country including the Baluch, Kurd,[57] and Arab communities, along with the many refugees from Afghanistan's endless wars.[58] Externally, MOIS is tasked to neutralize Iranian expatriate dissident organizations.[59] Concurrently, Iran shares a few problems with some of its adversary services, including domestic terrorism by ISIL (ISIS) on Iranian territory and infiltration into the country by such hostile non-state groups as al-Qaeda which has already penetrated the security services of some Sunni states.[60]

The basis for MOIS's internal security efforts, as with the independent efforts of its sister agencies, is an extensive informant system whose participants are expected to look for signs of dissent.[61] In addition, an extensive network of *Daftar-e Herasat* (Security Offices) across the country utilizes personnel reporting to MOIS across all public organizations, as well as governmental and educational agencies.[62] At a practical level, Herasat personnel impact hiring and firing decisions, monitor communications of those within the scope of their responsibilities, and act as informants against persons suspected of disloyalty.[63]

Working alongside the MOIS, the Basiji Mostazafan, now the largest militia in the world, conducts domestic counterintelligence using methods analogous to the old Communist Party system in Marxist–Leninist states.[64] The Basijis, sometimes dismissed because of their roughhewn unsophisticated origins, have become a major source of recruitment for both the Revolutionary Guard and the Security Police (PAVA). The Basiji have been described as ubiquitous throughout Iran by Saeid Golkar, with a massive network that serves as an

auxiliary that supports Iran's overall counterintelligence requirements. They also engage in ongoing indoctrination regarding the Velayat-e Faqih and violently suppress any open dissent against the regime. While organized across the Iranian state, the Basiji are generally associated with the rural and conservative communities that harbor resentment against urban elites and their perceived lack of piety. This widespread association was partially created by the Basiji organization's character, which is anchored in localism, and the family needs of the large numbers of volunteer teenagers and old men often utilized by the Basiji on a seasonal basis to accommodate the needs of agricultural labor.[65] The larger Basiji organization is built around resistance regions (Nahieh-e Basij), reporting to the IRGC provincial command (Sepah-e Ostani). These regions are divided into zones (Hozehale moghavamet-e Basij), which direct several resistance bases containing a variety of groups responsible for security and indoctrination.[66] Organizations relevant to the counterintelligence effort within these bases include the *Nasehin* groups, which, under the Council of Morality Policing in each base, enforce Islamic morality neighborhood by neighborhood. The Nasehin group includes an intelligence element (Shanasaei) which gathers information in support of passive surveillance. It includes members involved in intelligence collection (Mokhber Basij) through patrols that gather information about local developments and track down any relevant rumors.[67] In a way, the Basiji function as a malignant analog to the community policing ideal, but in this instance are intent on ferreting out any whisper of dissent.

CYBER'S CHALLENGE TO COUNTERINTELLIGENCE

The new dimension of cyber creates a most challenging arena for counterintelligence contests. Even in Western countries the counterintelligence space defined by the cyber domain is still often treated in the open literature and other narratives as an appendage rather than an integral element of analytical and operational intelligence disciplines. Perhaps that is due to an as yet incomplete integration of information technologies (ITs) into the counterintelligence practitioner's role. To date, cyber remains as a functionally discrete element of Iranian counterintelligence practice, most likely because Iran remains an economic and technological follower, rather than a leader, of the world's information technologies. Even those few discrete instances of world class Iranian cyber skills[68] do not remedy the larger problem of Tehran's having a second-rate information infrastructure.

The disastrous impact of the Stuxnet virus first awakened Iran to its cyber vulnerabilities and led to a response across its security sector. In 2010 Iran formally acknowledged its government-wide entrance into the field through the creation of cyber borders and the establishment of counterintelligence controls beginning with a Cyber Defense Command (Gharargah-e Defa-e Saiberi)

under the Artesh Passive Defense Organization that was tasked with defending the nation's information infrastructure. In 2012, a Supreme Council of Cyberspace (Shora-ye Ali-ye Fazo-ye Majazl) was decreed by Khamenei. Now directed by Mohammad Hassan Entezar, it coordinates government-wide efforts to establish and secure Iran's cyber domain,[69] with most activity focused on the suppression of any potential challenge to the *Vilayat-e*.[70] To secure its cyber borders, Tehran attempts to route all Internet communications through a Telecommunications Infrastructure Company[71] choke point, and secondarily, utilizing a variety of commercial systems that allow Iran to monitor normal internal communications between Iranians and the outside world.[72] Carnegie Endowment materials discussing Iran's cyber targeting of internal threats note that the techniques applied are well known, ranging from mapping Telegram accounts with Iranian phone numbers to targeting individuals with potentially dissident organizations with "spear phishing" campaigns. Likewise, to preclude any religious challenge to the regime's legitimacy, the Tehran regime, through the IRGC, targets and compromises the electronic communication and peer networks used by the authoritative Center for Services of Islamic Seminaries and the Islamic Propagation Office in Qom.[73] To manage the larger population, Iran has attempted to create some soft digital borders utilizing a National Information Network, or "Halal Internet," using greater connection speeds and steep price discounts that serve as tools of persuasion to encourage popular usage while concomitantly easing the challenge of monitoring digital activity within the country.[74]

Being able to effectively monitor social media to identify dissent is different from using information technologies to further intelligence analytics and operations on a national scale. The regime's clerical masters harbored growing suspicions about the religious reliability of those with the greatest technical skills, and sought to combat any opposition. One solution that worked, from a counterintelligence standpoint, was the creation of a compartmented system of tiered cyber operators executing assigned tasks furthering the *Vilayat* in cyber domains. This has created a somewhat amorphous system parallel to the dedicated government entities. These cyber operators, who often populate Iranian Security Forums, are contracted by the IRGC to code particular tasks, thereby taking advantage of their technical skills without risking penetration of government services through the hiring of politically or religiously unreliable personnel. The Revolutionary Guard can then administratively combine the products created by the contracted coders and those written in separate compartments to implement counterintelligence priorities.[75]

Formally, the Ministry of Interior administers a State Security Council (Shura-ye Aminiyat-e Keshvar) that coordinates the Ministry of Intelligence and the IRGC to manage Iran's internal security. But, in practical terms, the

Ministry of Interior under Mostafa Mohammad-Najjar plays a somewhat ancillary role in Tehran's security architecture, controlling ordinary crime as well as suppressing political dissent. The Interior Ministry includes Iran's Law Enforcement Forces (Niruha-ye Entezami-ye Jomhuri-ye Islami or NAJA) created in 1991 to incorporate urban police, the rural gendarmerie, and various revolutionary committees.[76] The NAJA, now under General Hosein Ashtari, are structurally rational in a Weberian sense, with a national leadership and a command headquarters in each province controlling local police stations. Typically, the stations incorporate at least one deputy for intelligence. The police recruit heavily from the Basiji, and roughly half the country's police force of approximately 100,000 consists of conscripts fulfilling their military service. NAJA's Intelligence and Public Security Police (PAVA) branch focuses on internal intelligence gathering in neighborhoods through networks of local informers (*Mokhber Mahali*).[77] In 2011, some cyber police organizations like FATA, under Brigadier General Kamal Hadianfar, began a more methodical surveilling of social media in order to target Internet crime and using the results as a basic roadmap to identify and suppress social and political dissent.[78] The fine granularity surveilling of social media platforms at this level is facilitated by the Police Electronic Services Office (Daftar-e Khademat-e Elekronik-e Entezami), sometimes called Police Plus Ten, which acts as an umbrella organization utilizing about forty thousand employees from private surveillance companies securing nearly five thousand neighborhoods.[79] Tehran's multiple security organs thus make it difficult to imagine any Iranian spaces devoid of regime informers.

Aside from dissent, internal corruption is probably the most significant underlying counterintelligence challenge facing Iran.[80] The pervasive corruption that replaced the long vanished élan of the Revolution now genuinely endangers the entire system of governance, including security forces, as institutional loyalty is being superseded by the desire for personal gain.[81] Corrupted individuals who knowingly violate Iranian law for personal economic gain are subject to witting or unwitting exploitation by foreign adversary intelligence services that seek entrée to Iran. The most common vector of corruption in Iran's NAJA is the illicit opium trade, since the bulk of Afghan opium production transits Iran at point or another.[82] Iran also hosts a variety of internal "mafias," particularly in sugar imports, hard currency, football clubs, and automobiles, often employing *aghazadeh* (children of important people) as corrupt facilitators.[83] Corruption and organized crime erode the integrity of any government but are particularly corrosive when undermining a Revolution that proclaims Islamic piety and claims to purify the hearts of men in the name of Allah.

Counterintelligence is a discipline with long horizons. The emerging horizon is digital, infused with artificial intelligence, and characterized by a

vanishing border between virtual and other realities. This is a challenge that Iran's Revolutionary government based on Ayatollahs is simply not capable of meeting. The existential counterintelligence threat facing the Partisans of Ali is a technological globalism that all of their piety cannot overcome.

REFERENCES

[1] See Michelle Van Cleave, "Strategic Counterintelligence: What Is It and What Should We Do With It?," *Studies In Intelligence* (Unclassified), Vol. 51, No. 2, pp. 1–15, and "What is Counterintelligence? A Guide to Thinking and Teaching About CI," *The Intelligencer: Journal of US Intelligence Studies,* Vol. 20, No. 2, Fall/Winter 2013, pp. 57–65. See also John Ehrman, "Toward a Theory of CI: What Are We Talking about When We Talk about Counterintelligence?," Central Intelligence Agency, Washington, DC, 24 August 2009; and James M. Olson, "The Ten Commandments of Counterintelligence: A Never-Ending Necessity," Central Intelligence Agency, Washington, DC, 14 April 2007. Also see, "Of Moles and Molehunters: A Review of Counterintelligence Literature, 1977–92," Central Intelligence Agency, Washington, DC, 1993.

[2] Robin Wright, *In The Name Of God: The Khomeini Decade* (New York: Touchstone, 1989), p. 110.

[3] Those who built the Revolution are sometimes referred to as the Burnt Generation (Nasl-e Sukhteh) due to the intensity of their struggle against the Shah's government and the Iran-Iraq War. MOIS consolidated power through a system of regional centers across Iran in the 1980s as the Khomeini government implemented the Revolution. See *Intelligence Newsletter,* No. 286, 18 April 1996. MOIS officers are sometimes referred to as Unknown Soldiers of the Imam.

[4] The *Rule of the Jurists* formed the basis for the Khomeini Revolution. See "The Islamic Republic's Art of Survival: Neutralizing Domestic and Foreign Threats," *Policy Focus* 125, Washington Institute for Near East Policy, June 2013, p. 11.

[5] "Iran's Clerical Spymasters," *Asia Times*, 31 July 2007.

[6] Wilfred Buchta, *Who Rules Iran*? (Washington, DC: Washington Institute of Near East Policy and Konrad Adenauer Stifung, 2000), p. 166. The Haqqani school itself was founded by the Hojjatieh, a semi-secret anti-Sunni society that technically rejects the *Vilayat-e Faqih* of post-revolutionary Iran. See "Shi'ite Supremacists Emerge from Iran's Shadows," *AsiaTimes,* 9 September 2005.

[7] "The Iranian Intelligence Services," 5 January 2010, *Note For News*, No. 200, French Centre for Research on Intelligence, Paris, available at www.cf2r.org, accessed 20 May 2010.

[8] "Who's Who," *Intelligence Online,* 4 April 1996.

[9] Counterintelligence was the responsibility of SAVAK's Eighth Directorate. Romania, as well as Russia, provided Iran with technology and tradecraft

training. See David Crist, *The Twilight War* (New York: Penguin Press, 2012), p. 82. According to Kaveh Moravej, the Eighth Directorate, using the cover of police officers, interviewed asylum seekers and immigrants. The Eighth was heavily dependent on human intelligence (HUMINT) as a core technique, and its personnel were drawn primarily from the Shah's military. Civilians in the Directorate were vouched for by existing personnel leading to significant problems of nepotism. Targeting Soviet personnel was not particularly sophisticated (tailing local Soviets from airports and noting that only intelligence officers were allowed to leave the embassy without accompaniment) and anchored in information sharing with the Foreign Ministry and flagged communications from liaison services in the CIA and MI6. See Kaveh Moravej, "The SAVAK And The Cold War: Counter-Intelligence And Foreign Intelligence (1957–1968)," Ph.D. Thesis, Faculty of Humanities, School of Languages, Linguistics And Cultural Middle Eastern Studies, University of Manchester, 2011. Notably, the loss of the CIA's ELINT Stations TACKSMAN I at Beshahr (not Busheir) and TACKSMAN II at Kabkan, roughly eight kilometers from Mashhad, were quite significant losses for U.S. collection of Soviet missile telemetry.

[10] Fallahian's immediate deputy, Bour Mohammedi, inherited the SAVAK's central filing system. Interior Security under Ali Rabii controlled the Interior Ministry and managed the network of regional MOIS Bureaus. The counter-espionage department was run by Mohammed Takari. The Technical Service under Mohammed Gharazi liaised with the Telecommunications Ministry. An entity referred to as Community Intelligence drew intelligence information from neighborhoods, mosques, and markets. See "Russian Style Overhaul," *Intelligence Online*, 18 April 1996.

[11] Some evidence indicates that Ahmad Chalabi may have been part of an Iranian disinformation operation intended to deceive the United States into attacking Iraq thereby eliminating a military threat to Iran. See "Ahmad Chalabi and His Iranian Connection," *Stratfor,* Worldview Geopolitics, 18 February 2004.

[12] A smaller number of 4000 professional staff operating in Iran may be more accurate for some purposes. Also note that MOIS officers who are assigned to a local Iranian Embassy typically serve three- to five-year terms.

[13] A Directorate of Overseas Affairs was responsible for MOIS branches abroad, with special emphasis on operations against the Peoples Mujahidin Organization. A Directorate of Foreign Intelligence and Liberation Movements participated in typical foreign espionage operations. A Directorate for Security ostensibly engaged in internal security but was primarily responsible for overseas assassinations of regime opponents. See *Intelligence Newsletter*, No. 286, 18 April 1996. The Peoples Mujahidin Organization is a Marxist organization founded in 1965 and dedicated to the overthrow of the Islamic Republic. Although considered a terrorist organization by the United States it has nonetheless provided apparently accurate information on Iran's nuclear program. "MOIS Structure," 28 February 2006, available at www.iranterror.

com/content/view/176/66. See also "The Iranian Intelligence Services," *Note For News,* No. 200.

[14] Khamenei appears to be coming to the end of his life, which will likely place the security organizations in the position of refereeing the transition to a new Supreme Leader.

[15] Clerical factions and their sycophants and cohorts in the various security services impact the rigor of police state constraints on civic society. The relative liberalism of a President Hassan Rouhani can conflict with Supreme Leader Khamenei's view of the *Vilayat*. When confronted with the possibility of genuine liberal reform a generation ago what was later known as a Parallel Intelligence Apparatus made up of rogue elements of the security services, acting as vigilantes for conservative clerics, emerged to crush the reformist impulse. See "Covert Terror: Iran's Parallel Intelligence Apparatus," *Iran Human Rights Documentation Center,* April 2009.

[16] This principle is also applicable to the Revolutionary Guard where formal rank is less important than client–patron relations. The IRGC also avoids an institution-wide system of ranking lest one individual gain inordinate power and authority. Ranks are relevant within different Guard entities rather than across the institution.

[17] "Cultural Intelligence for Military Operations: Iran," Marine Corps Intelligence Activity, *Cultural Field Guide on Iran,* Unclassified (Quantico, VA: U.S. Marine Corps), 2008. An Iranian intellectual named Jalal Ali Ahmad wrote an influential pamphlet on "Westoxication." The political vulnerability of the Baha'i is not helped by the fact that most of their leadership resides in the United States or Haifa, Israel.

[18] Dowrehs are circles of peer associates wherein Iranian social norms encourage open and frank conversation. With increasing social status, one can become a member of multiple Dowrehs where relaxed social standards can create security challenges.

[19] This structure was established 1 January 2005 replacing the old National Counterintelligence Center and now operating under the aegis of ODNI.

[20] See Michelle Van Cleave, "Strategic Counterintelligence: What Is It and What Should We Do With It?" For example, in one recent counterintelligence case Zahra Larijani, the daughter of the head of the Judiciary Sadiq Larijani, was arrested by IRGC Intelligence for compromising Iranian methods for obtaining nuclear relevant technologies via front companies to British intelligence (MI6). The British had apparently exploited her father's personal corruption after the Guard found Zahra had multiple bank accounts with significant funds at the ADB bank in Abu Dhabi and the Turkish Halkbank. Local surveillance apparently discovered her meeting with British nationals in Tehran and Tabriz and they likely thereafter located monies she held in foreign bank accounts. See "Iran: Daughter of Judiciary Head Accused of Espionage," *Middle East Monitor,* 24 October 2017.

[21] Mahan Abedin, "Iran Delivers Major Blow to the CIA," *Asia Times*, 1 December 2011, available at http://www.atimes.com/atimes/Middle_East/ML01Ak01.html. Apparently one wing of this CIA recruitment effort was

actively pitching persons with higher education in the hope they would eventually gain access to secret information. A priority collection target appeared to include methods by which Iran was evading sanctions as well as the country's financial and logistics networks.

[22] Iran's efforts to obtain nuclear weapons (sidestepping Khomeini's view that they were un-Islamic) may go back much earlier than generally thought. In 1980 conversations were apparently held between the Pakistani Army Chief of Staff General Aslam Beg and the head of the IRGC to assist Tehran in its nuclear programs in return for oil and weapons. See Owen Bennett Jones, *Pakistan: Eye of the Storm*, 3rd ed. (New Haven, CT and London: Yale University Press, 2009), p. 216.

[23] For example, the National Security Agency Special Collection Service (F6) targeted Iran in its Boundless Informant program.

[24] Wahidi's deputies included General Akbar Dianratr Far and General Ali Naghdi. See "Major Personnel Boost for Oghab-2," *Intelligence Online*, 11 May 2007.

[25] These threats included efforts by the United States under Pakistani auspices to put moles into the Iranian program. See *ibid*.

[26] A variety of local actors with their own political agenda as far apart as Azeri's and Baluchi's may be involved in such operations either directly or on behalf of foreign patrons.

[27] "Setback for Iran's Nuclear Watchdogs," *Intelligence Online*, 15 October 2009.

[28] "Iran's Ministry of Intelligence and Security: A Profile." A Report Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the Combating Terrorism Technical Support Office's Irregular Warfare Support Program, 2012, p. 34.

[29] Taeb studied jurisprudence in Qom and Mashhad and was on the faculty at Imam Hossein University. He also briefly served as espionage chief in MOIS. His deputy is General Mohammad Hossein Nehjat. The university of choice for the IRGC Counterintelligence Organization appears to be Imam Hadi University. See Saeid Golkar, "The Evolution of Iran's Police Forces and Social Control in the Islamic Republic," *Middle East Brief*, Crown Center for Middle East Studies, Brandeis University, July 2018.

[30] See "Rights Disregarded: Prisons in the Islamic Republic of Iran," *Iran Human Rights Documentation Center*, pp. 12–13, available at http://www.iranhrdc.org, accessed April 2018.

[31] *Ibid.*, p. 40.

[32] Iran Human Rights Documentation Center, October 2009, p. 30.

[33] "Iran Press: Counter-intelligence Centre Head Says Judiciary Protects System," *BBC Monitoring Middle East*, 28 September 2006.

[34] "Iran Exile Group: Khamenei Tightens Intelligence Grip," Reuters, 12 November 2009. Illustrative of that rivalry in a counterintelligence context was the public proclamation by MOIS that it alone had the professional skills to express an expert opinion as to who might be a foreign spy. Also see "Rivalry among Iranian Intelligence Bodies Spills Out Into the Open," *Al–Monitor,* 27 February 2018.

[35] A good general typology of counterintelligence is found in "A Counterintelligence Typology" by CDR (USNR, Ret) Kevin P. Riehle, *American Intelligence Journal*, NMIA, Vol. 33, No. 1, 2015, pp. 55–60. Riehle divides counterintelligence analysis into Foreign Intelligence Threat Analysis, assessing the threat to friendly interests by foreign intelligence activities; Counterintelligence Threat Analysis, advising positive intelligence collectors on methods to avoid foreign counterintelligence; Counterintelligence Operational and Investigative Analysis, which looks at methods to facilitate counterintelligence investigations, operations and information assurance; and Strategic Foreign Intelligence Analysis; that looks at foreign strategic decisionmaking and foreign intelligence activity.

[36] Executive Order 12333, 4 December 1981, amended by EO 13470, 4 August 2008. See also Title 50 USC Section 3003.

[37] Volker Foertsch defines it slightly differently claiming counterintelligence achieves its objectives by identifying, exploiting, and neutralizing the activities of adversary organizations and hostile states. Volker Foertsch, "The Role of Counterintelligence in Countering Transnational Organized Crime," *Trends in Organized Crime*, Winter 1999, p. 126.

[38] See "Iran's Ministry of Intelligence and Security: A Profile," pp. 24–26.

[39] "Is It Hard To Get Into Iran's Revolutionary Guard?" *Slate,* 23 September 2010.

[40] J. Matthew McImis, "The Future of Iran's Security Policy: Inside Tehran's Strategic Thinking," American Enterprise Institute, p. 15 Chart, May 2017.

[41] "The Islamic Republic's Art of Survival: Neutralizing Domestic and Foreign Threats," *Policy Focus* 125, Washington Institute for Near East Policy, June 2013, p. 10.

[42] The ability of the United States to collect information on Iran degraded faster than anyone might have imagined. The CIA initially attempted to run operations from Frankfurt, Germany (the so-called Tefran Station later replaced by an "Iran Station" run out of the U.S. Consulate in Dubai, where Iranian nationals apply for visas to the United States). But the 1983 bombing of the U.S. embassy in Beirut, Lebanon, crippled management from what was then called the Near East South Asia Division of the Directorate of Intelligence (DI) and the following year the kidnapping and eventual murder of Beirut Chief of Station William Buckley no doubt enlightened Iran respecting CIA intentions, some operations, and then current tradecraft. A network of Iranian military officers recruited by the CIA and run out of the Tefran Station, discovered by Iran and doubled to feedback false information, was publicly rolled up by Tehran in 1989. That large portions of Iran's military, while loyal to their nation, were hostile to Khomeini's Revolution was no secret. However, Iranian military officers, aware that they were generally perceived as disloyal to the Revolution, and so presumably taking all possible precautions, were nonetheless discovered and used for some months to feed deceptive information about Iran's tactical military planning back to their U.S. case officers, indicates that MOIS was able to run reasonably sophisticated

counterintelligence operations early on. See "Iran Broke C.I.A. Spy ring, U.S. Says," *The New York Times,* 8 August 1989.

[43] The arms merchant Manucher Ghorbanifar presenting a number of convenient defectors to the Defense Intelligence Agency (DIA) in the early 2000s is a case in point. There were enough red flags for the DOD's Counterintelligence Field Activity to begin an investigation, but Pentagon higher-ups shut down the investigation within a month, apparently believing that if they stopped looking for evidence that Ghorbanifar was controlled by Tehran it would save everyone political embarrassment. See "Did Iranian Agents Dupe Pentagon Officials?" McClatchy Newspapers, 5 June 2008.

[44] Defection from one foreign service to a different foreign service can directly impact the local security environment. For example, Vladimir Andreyevich Kuzichkin defected from the Soviet Embassy in Tehran and became a double agent for Great Britain. Kuzichkin was a rather significant coup for the British as he was a staff officer in KGB Directorate "S." His knowledge and documentation of Soviet domination of Iran's Communist Tudeh Party was ultimately provided by the British, for their own reasons, to the Khomeini government which used it to eviscerate the Iranian Communists. See Jack Anderson and Dale Van Atta, "Defection Hurt Iranian Communists," *The Washington Post,* 3 April 1985.

[45] Ashgari was apparently first approached by the CIA in Dubai would be the equivalent of an American Secretary of Defense defecting to a hostile service. See "The Ashgari Case: Defection and Damage Control," Stratfor, 14 March 2007. See also "The War in Libya and the Arab Spring," *Reason* 15 March 2007. At roughly the same time Shahram Amiri, a nuclear physicist from Malek Ashtar University in Tehran, defected while on Hajj, and an IRGC businessman defected in Georgia. The Amiri case illustrates the intrinsic ambiguity of defection. He came to the attention of the CIA in the late 1990s as part of a larger effort to encourage workers in Iran's nuclear program to defect. While he formally defected in 2009, his resettlement did not go well, and he returned to Iran in 2010. Amiri's original defection was apparently legitimate enough because once the Iranians had debriefed him and exploited the propaganda value of his return they executed him in 2015. But the lack of overt reprisals against his family would argue that there had been some negotiation in his debriefings. See Scott Ritter, "The Trouble With Defectors," *Harper's,* January 2017.

[46] *Iran's Cyber Threat: Espionage, Sabotage, and Revenge,* Colling Anderson and Karim Sadjadpour, "Internal Targets," Carnegie Endowment for International Peace, available at http://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134, accessed January 2018.

[47] "Another Iran Diplomat Defects to the Opposition," *Iran Times* 22 February 2011. Currently, the Intelligence Organization of the Revolutionary Guard carries the portfolio for monitoring Iranian diplomats. See *Iran: Procedural and Legal Information about Arrest and Detention Procedures by Different Security Organs*, Austrian Red Cross ACCORD, 12 June 2017.

[48] This dilemma is faced by all Second and Third World powers confronting First World services. For example, decades went by wherein most Second and Third world powers like Iran used encryption machines built by AG-Crypto in Switzerland and predictably the U.S. (along with Germany, Russia, and Israel) managed to compromise the encryption process at the point of manufacture. See "Memos Confirm Secret NSA Deal with Leading Cryptography Vendor," *Intelnews,* 31 July 2015.

[49] Iran, like many third world powers, had initially relied on diplomatic communications encryption supplied by the Swiss AG-Crypto firm and long compromised by the American National Security Agency (NSA) and the Germans (see Operation *Boris* and Hagelin backdoors). "The NSA-Crypto AG Sting," *Canada Free Press,* 31 December 2007. Additionally, the Echelon program alerted Tehran to additional risks respecting its diplomatic communications.

[50] Wahabuddin Ra'ees and Abdol Moghst Bani Kamal, "The Islamic Republic of Iran's Networking Diplomacy: The Role of Ahl-ul-Bayt World Assembly (ABWA)," *Intellectual Discourse,* Special Issue 2017, pp. 589–614.

[51] The PAVA or Public Security Police includes subordinate branches incorporating the Diplomatic Police and the Foreign Nationals and Immigrant Affairs Office to help track foreign security threats.

[52] Since the early 2000s the CIA has been trying to run agents into Iran from the Agency's Baghdad and Kabul Stations with little success. See Mathew M. Aid, *Intel Wars: The Secret History of the Fight Against Terror* (New York: Bloomsbury Press, 2012), p. 201.

[53] Human spotters are persons working on behalf of the security services who have memorized the facial features of many wanted individuals and look for them at international transit points. Newly-developed biometric systems will slowly reduce the need for such methods.

[54] "How Iranian Dissidents Slip through Tehran's Airport Dragnet," *The Christian Science Monitor,* 8 February 2010. Concerns about the compromising of electronic information system has led to the IRGC and MOIS watch lists being updated by hand and the updates delivered by courier every twelve hours, thus allowing a window for wanted persons to avoid immediate arrest.

[55] Both MOIS and the IRGC engage in constant operations against such terrorist organizations as Jundallah and its successor Jash Al-Adl that derive from marginalized Sunni populations in Sistan and Baluchistan, and are often supported by Western or Pakistani Special Operators of various types. See "Iran's Border Regions Seeing an Upsurge in Militant Activity," Middle East Institute, 25 January 2018.

[56] "The Geopolitics of Iran: Holding the Center of a Mountain Fortress," Stratfor, 16 December 2011. Iran's ethnic minorities (among them, the Turks, Kurds, and Lurs) are generally found on the periphery of the central Iranian plateau, thereby defining significant cultural features and being targets for exploitation by hostile intelligence services. See "Iran's Lurking Enemies Within," *Asia Times,* 8 January 2006.

[57] In addition to Azerbaijan, Israel's Mossad is particularly active in Iraqi Kurdistan.

[58] Iran's borders are much more porous than might be imagined which is problematic, as the name of the game in counterintelligence (in the words of James Olson) is to own the street. The IRGC has been forced to deploy its Saberin units to secure the country's northwestern and southeastern borders. See "Iran Struggles with Border Security," *Iran Pulse*, 18 February 2016. Iran has also exploited the opportunity for dragooning a good number of Afghans to fight on its behalf in Syria. The potential for foreign agents in such populations is an ongoing concern.

[59] "Special Report: Iranian Intelligence Regime Preservation," Stratfor, 21 June 2010, p. 7. Several distinct MOIS bodies recruit candidates for operations in the Gulf, Yemen and Sudan, Lebanon and Palestine, North Africa, Europe, South Asia and the Far East, North America, and Latin America. See "Insight: Iran-MOIS/IRGC Structure and Operations," *Global Intelligence Files,* Wikileaks, 17 March 2010, available at https://wikileaks.org/gifiles/docs/96/96828_insight-iran-mois-irgc-structure-and-operations-.html. See also "Special Series: Iranian Intelligence and Regime Preservation," Stratfor, June 2010.

[60] Justin R. Harber, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors," *International Journal of Intelligence and CounterIntelligence*, Vol. 22, No. 2, Summer 2009, pp. 221–236, at p. 223.

[61] Ariane M. Tabatabi, "Other Side of the Iranian Coin: Iran's Counterterrorism Apparatus," *Journal of Strategic Studies*, 2017, p. 11. Worth noting is that different kinds of informants are used for different purposes. Just as the police may use different types of informants for armed robbery cases than for drug cases, the various Iranian services have numerous categories of informants serving different purposes.

[62] "Significance of the Word '*Herasat*' Printed on a Seal of Summons [IRN41283.E]," *Document #1018189*. The word *Herasat* references civilian institutions and the term *Hefazat* is the analog in military and security organizations. *IRB—Immigration and Refugee Board of Canada*, available at https://www.ecoi.net/en/document/1018189.html, accessed 25 February 2018.

[63] Iran issued a national identity card in 2000 that in itself is reasonably sophisticated, and incorporated biometric data in 2013. That said, the document is frequently bypassed by bribery and other modalities. See *Iran Country Policy and Information Note Iran: Background Information, including Actors of Protection and Internal Relocation,* Home Office, December 2017, p. 56.

[64] Their own University Shahid Motahhari is also used by the IRGC for specialized training in security studies to accomplish their mission. See Saeid Golkar, "Organization of the Oppressed or Organization for Oppressing: Analyzing the Role of the Basij Militia of Iran," *Politics, Religion & Ideology*, Vol. 13, No. 4, December 2012, p. 459.

[65] "Cultural Intelligence for Military Operations: Iran," Marine Corps Intelligence Activity, *Cultural Field Guide on Iran,* Unclassified (Quantico, VA: U.S. Marine Corps, 2008).

[66] Basiji bases exist in all university faculty, and nearly half the university student seats are reserved for active Basiji. Membership in the Basiji is akin to Communist Party membership in the old Soviet bloc as a prerequisite for social advancement.

[67] Saeid Golkar, "Organization of the Oppressed or Organization for Oppressing: Analyzing the Role of the Basij Militia of Iran."

[68] External examples of Iranian cyber operations of counterintelligence value include malware under the umbrella name of "Cleaver," publicly disclosed by the American cyber security firm Cylance in 2014. Operations under "Cleaver" collected infrastructure vulnerabilities that could later be used in target packages exploited by Iran in any future conflicts. In addition to the United States, Saudi Arabia, and Pakistan a significant focus on South Korea's infrastructure suggested the harvesting of targets valued by North Korea as part of Iranian–North Korean military cooperation. See Stuart McClure, "Cylance Operation Cleaver Report," *Cylance*, November 2014, pp. 9–14.

[69] LTC Eric K. Shafa, "Iran's Emergence as a Cyber Power," *Strategic Studies Institute,* 20 August 2014, available at http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20n

[70] For example, Fox IT discovered 500 secure socket layer certificates fabricated to compromise 300,000 Iranian G-mail accounts via the hacking of Dutch DigiNotar servers. See "Hackers Spied on 300,000 Iranians Using Fake Google Certificates," *Computerworld,* 6 September 2011.

[71] "Iran's Web Spying Aided ByWestern Technology," *The Wall Street Journal*, 22 June 2009.

[72] For example, Chinese firms have sold Iran telecommunications equipment and software designed to geolocate Iranian voice and network communications users utilizing Chinese and American technologies. See "Special Report: Chinese Firms Help Iran Spy on Citizens," Reuters, 22 March 2012.

[73] *Iran's Cyber Threat: Espionage, Sabotage, and Revenge,* Colling Anderson and Karim Sadjadpour, "Internal Targets."

[74] See "Iran Country Report: Freedom On The Net 2017," *Freedom House*, June 2016–May 2017.

[75] Levin Gundert, Samil Chohanm, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed," *Recorded Future*, Cyber Threat Analysis, available at https://www.recordedfuture.com/iran-hacker-hierarchy/, accessed 15 May 2018. Also note that Gerdab.ir was a major contractor writing code used by the IRGC for internal censorship and monitoring of the population.

[76] Law enforcement forces appear to have a discrete counterintelligence unit, headed in 2000 by Abdolhosein Ramexani (no more recent name is in the public domain). See *Iran Country of Origin Information Report*, Home Office UK Border Agency, 31 August 2010, p. 31.

[77] See Saeid Golkar, "Iran's Coercive Apparatus: Capacity and Desire," *The Washington Institute for Near East Policy*, 5 January 2018. Iran uses a system of color codes for internal security; white—normal, gray—unorganized nonviolent opposition, yellow—organized opposition disrupting public order, and red—armed national revolt.

[78] FATA within just a couple of years had established a presence in all thirty-one provinces and fifty-six cities across Iran.

[79] Saeid Golkar, "Iran's Coercive Apparatus: Capacity and Desire." Police Electronic Services also issue drivers licenses and passports.

[80] Iran Corruption Report 2017, GAN Business Anti-Corruption Portal, available at https://www.business-anti-corruption.com/country-profiles/iran, accessed 25 February 2018.

[81] Iran recently was ranked at 130th out of 175 nations in terms of perceived public-sector corruption. See https://tradingeconomics.com/iran/corruption-rank, accessed 18 February 2018.

[82] "The Scourge of Opiates: The Illicit Narcotics Trade in the Islamic Republic of Iran," *Trends in Organized Crime,* No. 14, 2011, p. 327. Three major smuggling routes transit Iran from Afghanistan. The northern route moves through Razari and south Khorasan province transporting narcotics destined for Russia. The southern route via Sistan and Baluchistan provinces is for opiates destined for Bander Abbas that eventually move to Europe and North America; and the Hormozgan route. The most common trafficking routes go from Tehran to Azerbaijan and Urumiyeh province near Turkey. Compounding the opium problem is the emergent production and trafficking of Amphetamine Type Stimulants (ATS) including methamphetamine known locally as *Shisheh*. See "Drug Trafficking And Border Control Situational Analysis," United Nations Office on Drugs and Crime Country Programme for Islamic Republic of Iran 2011–2014. Despite its other confrontations with external powers Iran has good relations with foreign drug enforcement police. Iran stops eight times more opium than any other country. "The West's Stalwart Ally in the War on Drugs: Iran (Yes, That Iran)," *The New York Times*, 11 October 2012.

[83] "How Do Iran's 'Corrupt Networks' Operate?" *Al Monitor,* 13 February 2018. The basis for police corruption is less relevant than the fact of police corruption which can be exploited by adversary intelligence services for operational advantage.